

**SYSTEMS AND METHODS FOR PROVIDING DYNAMIC NETWORK
AUTHORIZATION, AUTHENTICATION AND ACCOUNTING**

5 **CROSS-REFERENCE TO RELATED APPLICATIONS**

 This application is a continuation-in-part of copending U.S. Patent Application
Serial No. 09/458,569, filed on December 8, 1999, titled "Systems And Methods For
Redirecting Users Having Transparent Computer Access To A Network Using A
Gateway Device Having Redirection Capability". This application also claims priority
10 from U.S. Application Serial No. 09/458,602, filed December 8, 1999, titled "Systems
and Methods For Authorizing, Authenticating and Accounting Users Having Transparent
Computer Access To A Network Using A Gateway Device," U.S. Provisional
Application Serial No. 60/161,182, filed October 22, 1999, titled "Systems and Methods
for Dynamic Bandwidth Management on a Per Subscriber Basis in a Computer
15 Network," U.S. Provisional Application Serial No. 60/160,890, filed October 22, 1999,
titled "Systems and Methods for Creating Subscriber Tunnels by a Gateway Device in a
Computer Network," U.S. Provisional Application Serial No. 60/161,139, filed October
22, 1999, titled "Information And Control Console For Use With A Network Gateway
Interface," U.S. Provisional Application Serial No. 60/161,189, filed October 22, 1999,
20 titled "Systems and Methods for Transparent Computer Access and Communication with
a Service Provider Network Using a Network Gateway Device," U.S. Provisional
Application Serial No. 60/160,973, filed October 22, 1999, titled "Systems and Methods
for Enabling Network Gateway Devices to Communicate with Management Systems to
Facilitate Subscriber Management," U.S. Provisional Application Serial No. 60/161,181,
25 filed October 22, 1999, titled "Gateway Device Having an XML Interface and Associated
Method," and U.S. Provisional Application Serial No. 60/161,093, filed October 22,
1999, titled "Location-Based Identification and Authorization for use With a Gateway
Device." All of the above applications are incorporated by reference in their entirety.

FIELD OF THE INVENTION

The present invention relates generally to systems and methods for controlling network access, and more particularly, to systems and methods for establishing dynamic user network access.

5

BACKGROUND OF THE INVENTION

User access to computer networks has traditionally been based upon a two step authentication process that either provides a user total network access, or refuses the user any access whatsoever. In the first step of the process, a user establishes a
10 communication link with a network via a telephone line, dedicated network connection (e.g., Broadband, Digital Signal Line (DSL)), or the like. In the second step of the authentication process, the user must input identification information to gain access to the network. Typically, the input identification information includes a user name and password. Using this information, the network or service provider verifies that the user is
15 entitled to access the network by determining whether the identification information matches subscriber information contained in a subscriber table (or database) that stores identification information for all users authorized to access the network. Where user input information matches subscriber data in the subscriber table, the user is authorized to access any and all services on the network. On the other hand, if the user input
20 identification information fails to match subscriber data in the table, the user will be denied access to the network. Thus, once a user's identity is compared to data stored within a subscription table, the user is either entitled network access, or denied access altogether. Furthermore, where the user is authorized access to the network, the user is typically authorized to access any destination accessible via the network. Therefore,
25 conventional authentication of users is based on an all-or-nothing approach to network access.

In many conventional network access applications, such as in conventional Internet access applications, the subscriber database (or table) not only stores data corresponding to the identity of subscribers authorized to access the network, but also
30 stores information that can vary based upon the particular subscriber. For instance, the subscriber database can include subscriber profiles that indicate the type of access a

5

10

20

25

5

SUMMARY OF THE INVENTION

30

SECRET

According to yet another aspect of the invention, the method includes updating
25 the source profile database when a new source accesses the network. Additionally, the
method can include maintaining in the source profile database a historical log of the
source's access to the network. Moreover, the attribute associated with the source can be
based upon a MAC address, User ID or VLAN ID associated with the source computer
from which the request for access to the network was transmitted. According to yet
30 another aspect of the invention, receiving at the gateway device a request from a source
for access can include the step of receiving a destination address from the source.

According to another embodiment of the invention, there is disclosed a system for selectably controlling and customizing access, to a network, by a source, where the source is associated with a source computer, and wherein the source computer has transparent access to the network via a gateway device and no configuration software
5 need be installed on the source computer to access the network. The system includes a gateway device for receiving a request from the source for access to the network, and a source profile database in communication with the gateway device and located external to the gateway device, wherein the source profile database stores access information identifiable by an attribute associated with the source, and wherein the attribute is
10 identified based upon a data packet transmitted from the source computer and received by the gateway device. The system also includes a AAA server in communication with the gateway device and source profile database, wherein the AAA server determines if the source is entitled to access the network based upon the access information stored within the source profile database, and wherein the AAA server determines the access rights of
15 the source with the access rights defining the rights of the source to access destination sites via the network.

According to one aspect of the invention, the packet received by the gateway device includes at least one of VLAN ID, a circuit ID, and a MAC address. Additionally, according to another aspect of the invention, the source profile database includes a
20 remote authentication dial-in user service (RADIUS) or a lightweight directory access protocol (LDAP) database. Furthermore, the source profile database can include a plurality of source profiles, wherein each respective source profile of the plurality of source profiles contains access information. According to the invention, each respective source profile can also contain historical data relating to the duration of network access
25 for use in determining the charges due for the network access. According to yet another aspect of the invention, the source profile database can be located within the AAA server.

According to another embodiment of the present invention, there is disclosed a method for redirecting a source attempting to access a destination through a gateway device, wherein source is associated with a source computer, and wherein the gateway
30 device enables the source to communicate with a network without requiring the source computer to include network software configured for the network. The method includes

receiving at the gateway device a request from the source to access the network,
 identifying the source based upon an attribute associated with the source, and accessing a
 source profile database located external to the gateway device, where the source profile
 database stores access rights of the source. The method further includes determining the
 5 access rights of the source based upon the identification of the source, wherein the access
 rights define the rights of the source to access destination sites via the network.

According to one aspect of the invention, accessing a source profile database
 includes accessing a source profile database that includes a remote authentication dial-in
 user service (RADIUS), or a lightweight directory access protocol (LDAP) database.

10 According to another aspect of the invention, the method can include assigning a location
 identifier to the location from which requests for access to the network are transmitted,
 wherein the location identifier is the attribute associated with the source. The method can
 also include updating the source profile database when a new source accesses the
 network, and maintaining in an accounting database a historical log of the source's access
 15 to the network, wherein the accounting database is in communication with the source
 profile database.

According to yet another aspect of the invention, receiving at the gateway device
 a request from a source for access can include the step of receiving a destination address
 from the source. Moreover, determining if the source computer is entitled to access the
 20 destination address can further include denying the source computer access where the
 source profile indicates that the source computer is denied access. Determining if the
 source is entitled to access the network can also further include directing the source to a
 login page when the source profile is not located within the source profile database.

According to yet another embodiment of the invention, there is disclosed a system
 25 for enabling transparent communication between a computer and a service provider
 network. The system includes a computer, and a network gateway device in
 communication with the computer for connecting the computer to a computer network,
 where the network gateway device receives source data that represents a user attempting
 to access said computer network. The system also includes a service provider network in
 30 communication with the network gateway device, where the service provider network
 includes an authentication server located external to the network gateway device and in

5

10

20

FIG. 1 is a block diagram of a computer system that includes a AAA server for authenticating, authorizing and accounting sources accessing networks and/or online services, according to one embodiment of the present invention.

5

10

20

30

multiplexing the signals received from the plurality of computers onto a link to the gateway device 12. Depending upon the medium by which the computers 14 are connected to the access concentrator, the access concentrator 16 can be configured in different manners. For example, the access concentrator can be a digital subscriber line access multiplexer (DSLAM) for signals transmitted via regular telephone lines, a cable head end (a Cable Modem Termination Shelf (CMTS)) for signals transmitted via coaxial cables, a wireless access point (WAP) for signals transmitted via a wireless network, a switch, or the like.

The computer system 10 further includes a AAA server 30 that dynamically authenticates and authorizes user access, as explained in detail below, such that users are subjected to a AAA process upon attempting to gain access to a network through the gateway device 12. Finally, as is shown in FIG. 1, the computer system 10 typically includes one or more routers 18 and/or servers (not shown in FIG. 1) to control or direct traffic to and from a plurality of computer networks 20 or other online services 22.

While the computer system 10 is depicted to have a single router, the computer system 10 can have a plurality of routers, switches, bridges, or the like that are arranged in some hierarchical fashion in order to appropriately route traffic to and from the various networks 20 or online services 22. In this regard, the gateway device 12 typically establishes a link with one or more routers. The routers, in turn, establish links with the servers of the networks 20 or online services 22, based upon the user's selection. It will be appreciated by one of ordinary skill in the art that one or more devices illustrated in FIG. 1 may be combinable. For example, although not shown, the router 18 may be located entirely within the gateway device 12.

Users and computers attempting to access a network 20 or online service 22 via the gateway device 12 are referred to hereinafter as sources. According to AAA methods and systems of the present invention, a source attempting to access a network via the gateway device 12 is authenticated based on attributes associated therewith. These attributes can include the identity of a particular user or computer, location through which access is requested, requested network or destination, and the like. As is explained in detail in the Gateway Device Application, these attributes are identified by data packets transmitted to the gateway device 12 from the computers through which access is

5

10

20

individual rights of each user, as the rights are associated with the computer (e.g., identified by MAC address), rather than with the respective users.

The authentication of sources via an attribute associated with the source is performed by the AAA server 30, illustrated in FIG. 1. The AAA server 30 stores source profiles corresponding to sources identified by the AAA server 30. According to one aspect of the present invention, the AAA server 30 is located entirely within the gateway device 12. According to another aspect of the invention, the AAA server 30 can comprise a plurality of components, at least some of which are external to the gateway device 12, or alternatively, the AAA server 30 can be located entirely external to the gateway device 12. For example, the location of the AAA server 30 may be such that the gateway device 12 communicates with the AAA server 30 via internet protocol. According to one embodiment of the invention, the AAA server 30 can be maintained by an ISP, which identifies sources authorized to communicate with the network via the ISP. Therefore, it will be appreciated that the AAA server 30 may be located at any internet address and stored on any computer accessible via internet protocol.

According to one aspect of the invention, a separate source profile exists for each source accessing the system. Source profiles are maintained in a source profile database, which may be an internal component of the AAA server 30, an external component of the AAA server 30, or a separate component in communication with the AAA server 30. Preferably, the source profile database is located external to the gateway device and network to alleviate administrative burden on the network so that the network does not have to set up and maintain separate authentication databases on each network or gateway device. This is also preferable because each gateway device 12 allows a finite number of users to access the network, which requires multiple gateway devices to accommodate a large number of sources. Secondly, administering and maintaining one consolidated database of authentication data is easier than multiple smaller databases. Lastly, locating the source profile database external to the local network can allow an ISP or third party provider to maintain the confidentiality of the information stored within the database and maintain and control the database in any manner the third party provider so desires.

The source profile database may comprise programmable storage hardware or like means located on a conventional personal computer, mainframe computer, or another suitable storage device known in the art. Additionally, the means for comparing the received data to the data within the database can comprise any software, such as an executable software program, which can compare data. For example, the AAA server 30 may store source profiles on a hard drive of a personal computer, and the means for comparing the received source data to the source profiles resident on the computer can include computer software, such as Microsoft Excel (Microsoft Excel is a trademark of Microsoft Corporation, Redmond, Washington). According to another embodiment of the invention, the AAA server 30 or source profile database can comprise a Remote Authentication Dial-In User Service (RADIUS) or a Lightweight Directory Access Protocol (LDAP) database, which are well known to those of skill in the art.

ATL01/10823107v2

According to another aspect of the invention, where the source cannot be identified, the source may be directed to a login page in order to gather additional information to identify the source. For instance, the information may be entered with the aid of a webpage, a pop-up control panel or user interface, which can open when the source initially connects to the gateway device 12, as effectuated by a home page redirection capability, described herein and in U.S. Patent Application, Serial No. 09/458,569, filed December 8, 1999, entitled "Systems And Methods For Redirecting Users Having Transparent Computer Access To A Network Using A Gateway Device Having Redirection Capability" (referred to hereinafter as the "Redirection Application"), in U.S. Patent Application, Serial No. 09/458,579, filed December 8, 1999, entitled "Systems And Methods For Redirecting Users Having Transparent Computer Access To A Network Using A Gateway Device Having Redirection Capability," and in U.S. Patent Application, Entitled "Systems and Methods for Redirecting Users Attempting to Access a Network Site," filed concurrently herewith, inventors Joel Short and Florence Pagan, the contents of each of which are incorporated herein by reference.

According to one aspect of the invention, the AAA server 30 can identify the source in communication with the gateway device in a manner that is transparent to computer users. That is, according to one aspect of the invention, a user will not be required to input identification information, reconfigure the source computer or otherwise change the source computer's primary network settings. Furthermore, no additional configuration software will have to be added to the source computer. After a packet is received by the gateway device, attributes identified by the data packet can be compared with the data contained in the source profile database. Therefore, in addition to not requiring the reconfiguration of computers accessing the network, AAA servers of the present invention have the ability to authenticate sources without requiring interactive steps by the computer user, such as the entering of a user ID. For instance, the AAA server 30 may automatically identify the source based upon a MAC address, so that authorization of the source can be readily determined. Therefore, it will be appreciated that the AAA server 30 can determine the user, computer, or location from which access is requested by comparing the attributes associated with the received data packet (such as in a header of the data packet) with data drawn from the source profile database. As will

09693060-100000

be described below, the access rights associated with the source may also be stored within the source profile database so that the system and method of the present invention can dynamically authorize access to particular services or destinations.

Once the source has established the network service connection via the authentication process discussed above, and a tunnel has been opened to facilitate a communication line between the source computer and a network, the gateway device 12 communicates with the AAA server 30 to assemble source profile information, or source-specific data. The source profile information that the gateway device assembles may include a MAC address, name or ID, circuit ID, billing scheme related data, service level data, user profile data, remote-site related data, and like data related to the source. As such, the AAA server 30 can transmit to the gateway device 12 any requisite information relating to the source's authorization rights and use of the network, as is next explained in detail.

In addition to authenticating users, the AAA server 30 of the present invention provides an authorization function, in which the source access rights are determined. The present invention enables dynamic authorization of sources, such that each source might have different respective network usage or access rights. After authentication, the AAA server 30 compares the attributes of the source with the access rights of the source associated with the user, computer, location or attribute(s). The access rights may be stored within the source profile database or within a separate subscription database located internal or external to the gateway device 12. Therefore, separate databases may be utilized, where one stores identification information on sources for authentication, and another database stores the access rights of those sources that have been authenticated. However, because the profiles of all sources, identified by attribute or a combination of attributes, are stored in a source profile database, it may be advantageous to locate information regarding access rights in the source profile database, which already contains information regarding each authenticated source, as described above.

According to one aspect of the invention the source profile database stores information defining the access rights of a source. For example, a source profile database may contain information indicating that a source having a particular MAC address has purchased pre-paid access, or that a given circuit ID has free access or unlimited access.

Guests in a particular room or rooms of a hotel, for example, suites and penthouses, may receive free unlimited Internet access. Therefore, access rights can be available contingent upon the source's location (e.g. room) or location status (e.g. suite). In this event, no further identification is required, as the location from which the source is requesting access is known to the gateway device and stored in the source profile database.

In addition to storing information concerning what each source is authorized to access, the source profile database can also include specialized access information associated with a particular source, such as the bandwidth of the source's access, or a homepage to which the source should be directed. For example, a user accessing the network from a penthouse may receive a higher access baud rate than someone accessing the network from a typical hotel room. For example, where a user is transparently accessing the gateway device from a hotel room, the hotel network administrator may enter user access information into the source profile database based upon access rights associated with a room in the hotel. This can also be done automatically by the gateway device or a local management system, such as a hotel property management system, when the user checks into his or her room. Additionally, the user may establish the information to be contained within the source profile database upon first accessing the gateway device. For instance, a new user may be directed to enter a credit card number, e-wallet account information, pre-paid calling card number or like billing information to obtain access to the system. A source profile can also include historical data relating to a source's access to the network, including the amount of time a source has accessed the network. Specialized access or accounting information contained within the source profile database may be established by the system administrator, or by the source who has purchased or otherwise established access to the network.

According to one aspect of the invention, the authorization capability of the AAA server 30 can be based upon the type of services the source is attempting to access, such as a destination address, identified by the gateway device 12 based upon data received from the source computer. The destination can be a destination port, Internet address, TCP port, network, or the like. Moreover, the authorization capability of the AAA server 30 can be based upon the content type or protocol being transmitted. According to the

system and method of the present invention, each packet can be filtered through the selective AAA process, so that any or all sources can be authorized access to a particular destination based on the access rights associated with the respective sources. Therefore, according to the present invention, each time the source attempts to access a different

5 destination, the source is subject to the AAA, so the source may be prevented access from a particular site the AAA server **30** deems inaccessible to the source based upon the source's authorization. Alternatively, the AAA method according to the present invention allows some or all sources to connect directly to a specific site, such as credit card or billing servers for collecting billing information, which can collect payment or

10 billing information so that the source profile can be updated and the source thereafter authorized access to networks. According to the system and method of the present invention, a source's authorization can also depend upon objective criteria, such as a specific time, so that the session can be terminated at a specific time, after a specific time has elapsed, or according to other dynamic information determined by the network

15 provider. Furthermore, authorization can be associated with a combination of attributes. For example, a user may be authorized access to a network where the user has input the user's identification and has accessed the network from a particular room. Such a requirement could prevent unauthorized users also staying in a particular room from obtaining network access. Therefore, AAA can be based upon the origination,

20 destination, and type of traffic.

By way of further explanation, a flow chart of the operation of the AAA server **30** will be described with respect to FIG. 2, according to one aspect of the invention. In operation, a source computer requests (block **200**) access to a network, destination, service, or the like. Upon receiving a packet transmitted to the AAA server **30**, the AAA

25 server **30** examines the packet to determine the identity of the source (block **210**). The attributes transmitted via the packet are temporarily stored in the source profile database so that the data can be examined for use in determining authorization rights of the source. The attributes contained in the packet can include network information, source IP address, source port, link layer information, source MAC address, VLAN tag, circuit ID,

30 destination IP address, destination port, protocol type, packet type, and the like. After

Once a source profile has been determined by accessing the authorization rights stored in the source profile database, three possible actions can result. Specifically, once a source's authorization rights have been retrieved the AAA server **30** may determine a source to have access **222**, to be pending or in progress **224**, or to not have access **226**. First, a source is deemed valid (i.e., to have access) where the source profile database so states. If a source is determined to be valid, the source's traffic can be allowed to proceed out of the gateway device to the networks or online services the user associated with the source wishes to access (block **230**). Alternatively, the source may be redirected to a portal page, as described in the Redirecting Application, prior to being allowed access to the requested network. For example, a user may be automatically forwarded to a user-input destination address, such as an Internet address, for example, where a user has free access associated with the user's hotel room. Alternatively, this may occur where the user has already purchased access and the user has not exhausted available access time. Furthermore, an accounting message may be initiated **230** to log the amount of time the user is utilizing the gateway device such that the user or location may be billed for access.

ATL01/10823107v2

have access **226** so that the user is not permitted to access a destination via the network (block **260**).

Referring now to the accounting function of systems and methods of the present invention, upon authorizing a source network access, the AAA server **30** can register an accounting start to identify that the source is accessing the network. Similarly, when the source logs off or terminated the network session, an accounting stop can be registered by the AAA server **30**. Accounting starts or stops can be identified by the gateway device **12** or by the AAA server **30** upon a source's authentication or authorization to access a desired destination. Furthermore, accounting starts or stops can be registered in the source profile, or can be stored in a database separate from the AAA server **30** and located external to the network. Typically, accounting starts and stops include time stamps that indicate the amount of time a source has been accessing the network. Using this data, the time between the accounting start and accounting stop can be tallied so that the source's total connection time may be computed. Such information is valuable where the source is charged by an increment of time, such as an hour. A billing package, as are well known in the art, could then tally a user's total time accessing the network over a set period, such as each month, so that a bill can be created for the source. Because networks and ISPs often may charge a set rate for a specific duration of time (i.e., flat rate pricing), such as a month, regardless how much time is being spent accessing the network, accounting stops and starts may not be required for billing purposes. Nevertheless, accounting starts and stops may generally be recorded by the network provider or ISP for usage statistics.

An ISP or similar access provider would additionally benefit from being able to track subscriber's use of the ISP to establish bills, historical reports, and other relevant information. Preferably, the AAA server **30** is in communication with one or more processors for determining any fees which may be charged to the source, or due from the source, for network access or services. The AAA server **30** retrieves the historical accounting data in a real time basis or after a specific interval of time has elapsed. Preferably, the AAA server **30** retains such data in an easily accessible and manipulatable format such that the access provider (e.g., ISP) can produce reports representative of any desired type of historical data. For example, to project future use of the access provider,

the AAA server 30 produces reports tallying the number of users accessing the Internet at certain time periods and from specific locales. Moreover, where the access provider provides alternative access to users, such as charging for faster connections (i.e., higher baud rate) for additional fees, the access provider may wish to analyze historical data using the AAA server 30 to best meet future customer demands. Such data may relate to network sessions currently on-going, the duration of those sessions, the bandwidth currently being used, the number of bytes that have been transferred and any other pertinent information. The AAA server 30 may be implemented using well known programs, such as Eclipse Internet Billing System, Kenan Broadband Internet Billing Software (manufactured by Lucent Technologies), or TRU RADIUS Accountant.

It will be appreciated that the AAA server 30 can dynamically account source access to a network in the same manner in which access is customizable on a source by source basis. That is, the AAA server 30 can maintain accounting records that vary depending upon the identity of a source, source location, source requested destination, or the like. Like the access or authorization rights, this information can be maintained in the source profile database or a similar accounting database. For instance, the AAA server 30 may determine that a particular source is only charged for accessing particular sites, and will only register an accounting site when those particular sites are accessed. Therefore, the AAA server 30 will identify account information stored in the subscriber's source profile to determine accounting starts, accounting stops, billing rates, and the like.

Many modifications and other embodiments of the invention will come to mind to one skilled in the art to which this invention pertains having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.